

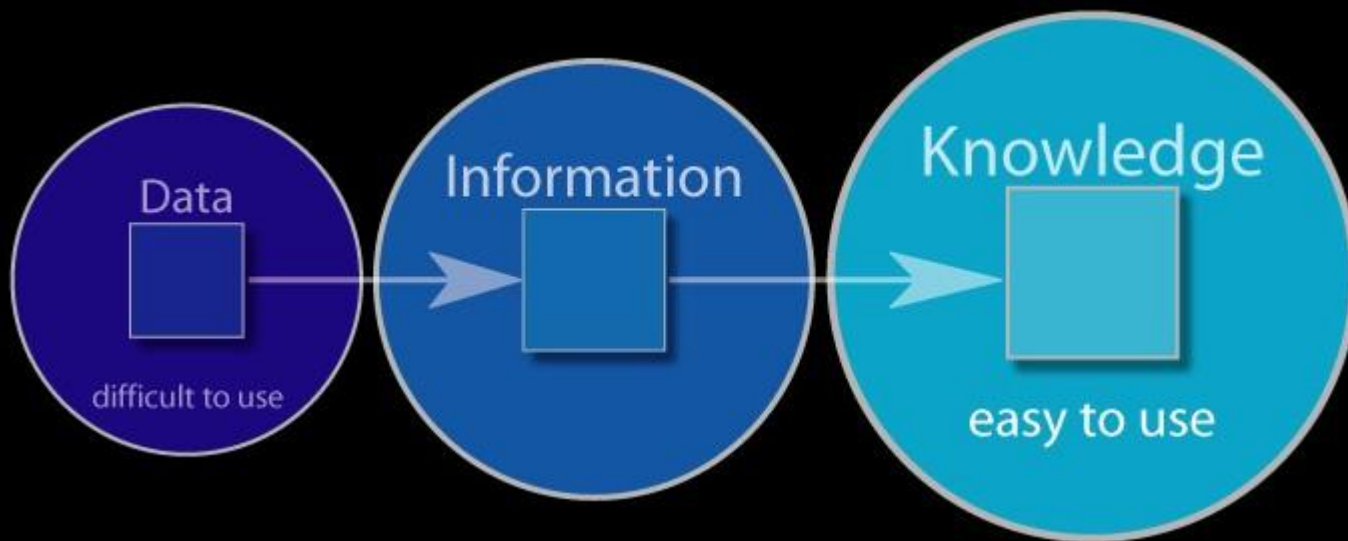
## YEAR 6 REVIEW

**Center for the Representation of Multi-Dimensional Information**

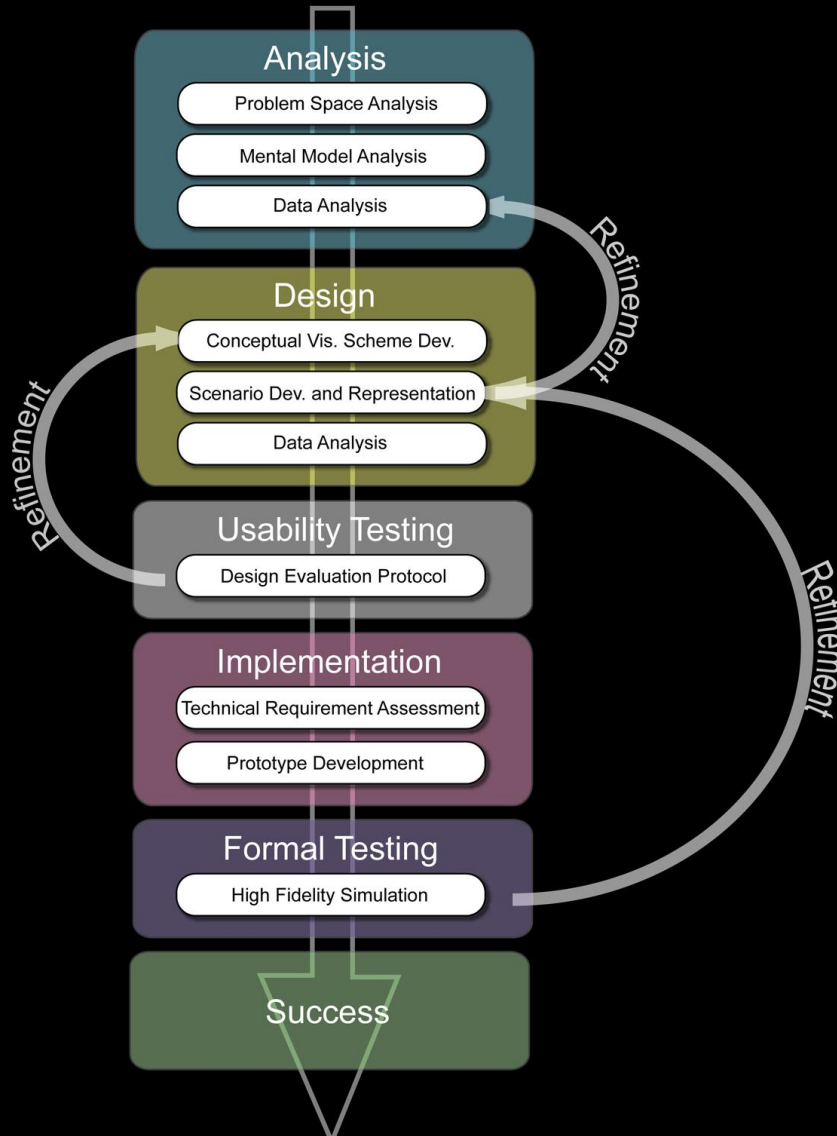
**University of Utah**

[www.cromdi.utah.edu](http://www.cromdi.utah.edu)

# Data to Knowledge Through Visualization



# Full Cycle Development



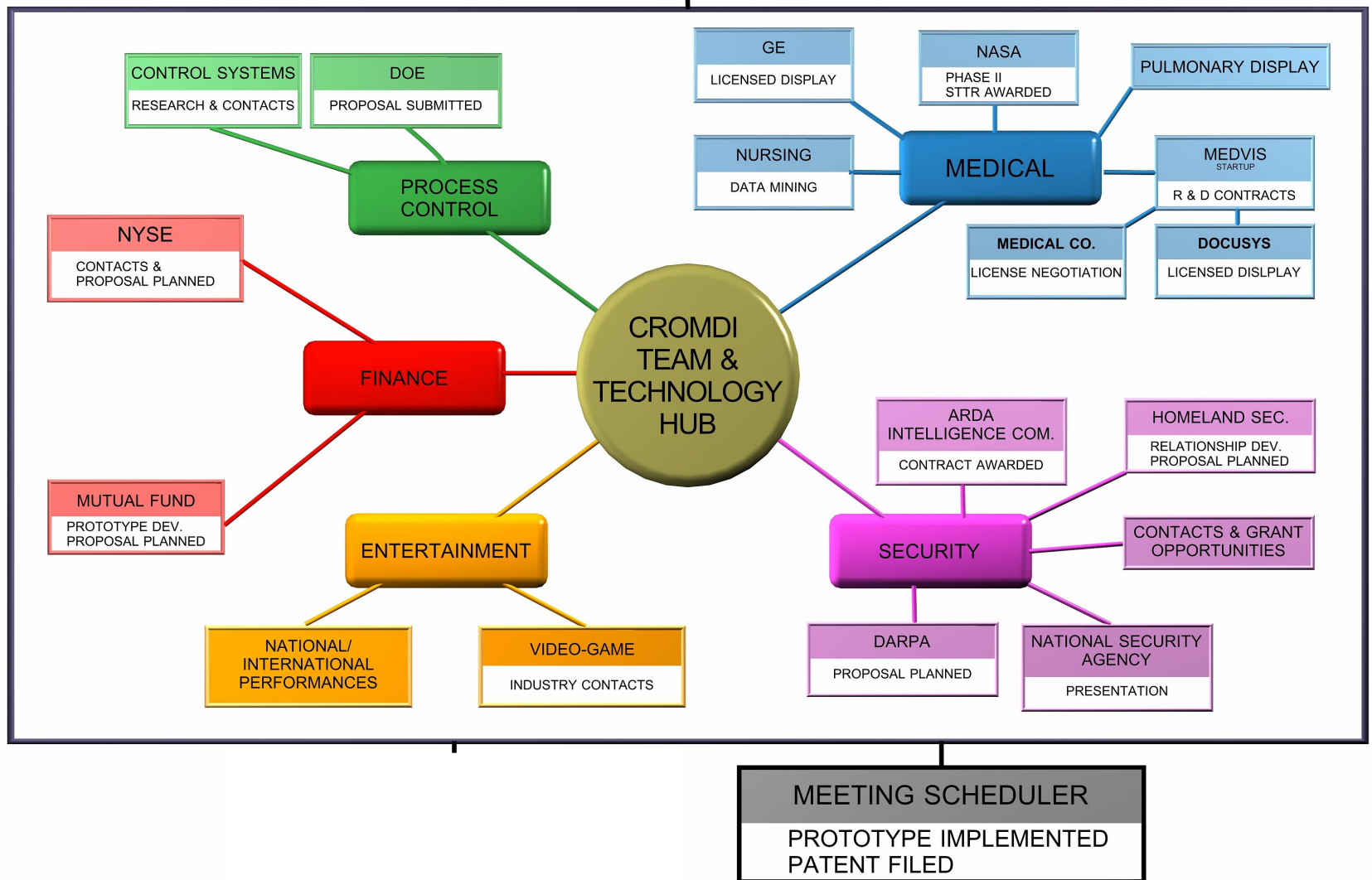
# CROMDI History

- 5 Year COE
- Complete Interdisciplinarity
- Commercialization & Business Success
  - 5 licensees and sublicenses, Spin-off company
- Broad funding Over \$5.3 million
  - Federal, State Grants, Military Contracts, Industry support
- 10 years experience
- Multiple Awards and Recognitions

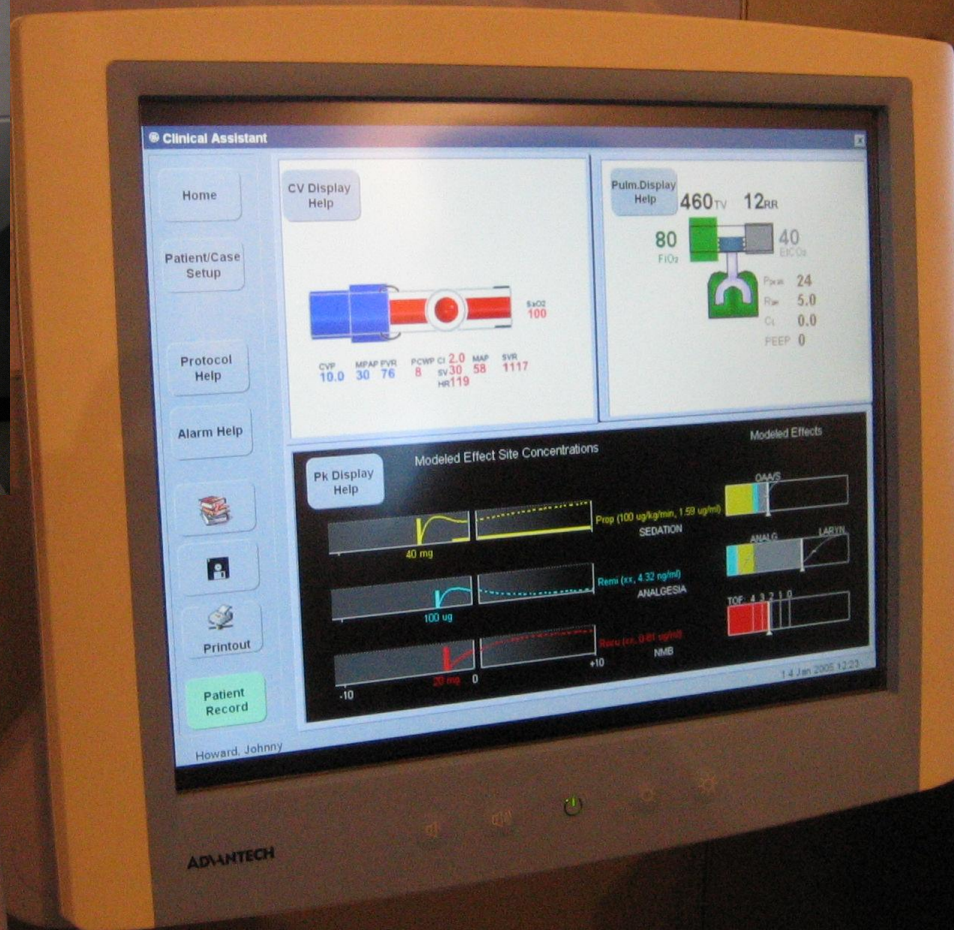
# CROMDI ACCOMPLISHMENTS

INTERDISCIPLINARY COLLABORATION METHODOLOGY

NSF GRANT SUBMISSION



# GE Medical



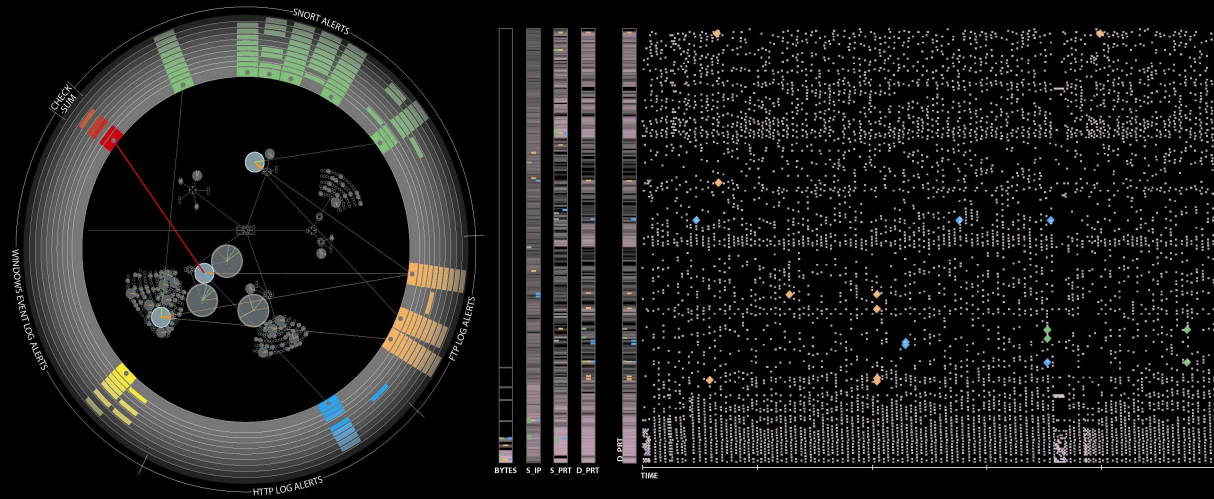
# Summary

- 3 Products
  - VisAlert
  - VisAlert NOCC
  - Meeting Scheduler
- Combined market size \$400 Million
- Combined 7 Year EBITDA \$43 Million
- Patents Filed
- First product in 6 months

# Technologies

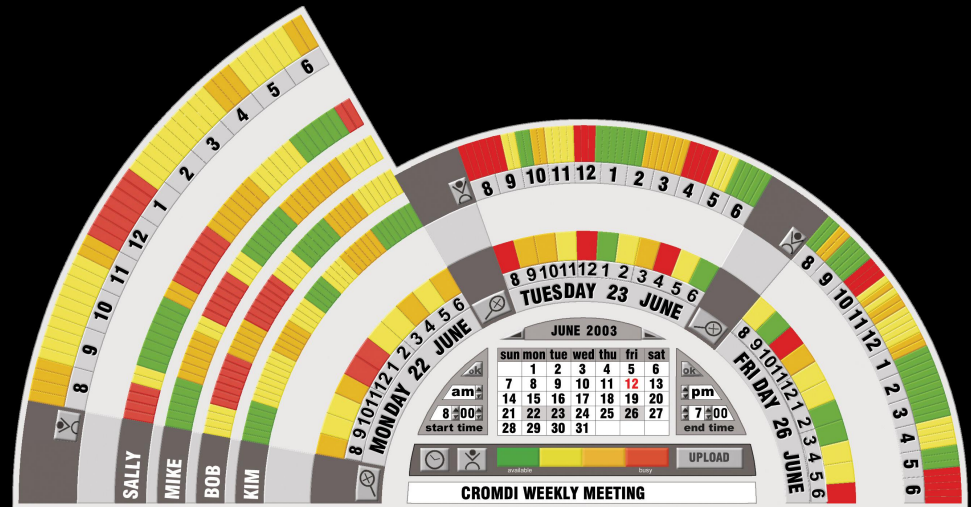
- VisAlert

- Network Security tool
- Provisional Patent
- Prototype tested
- Government Partners



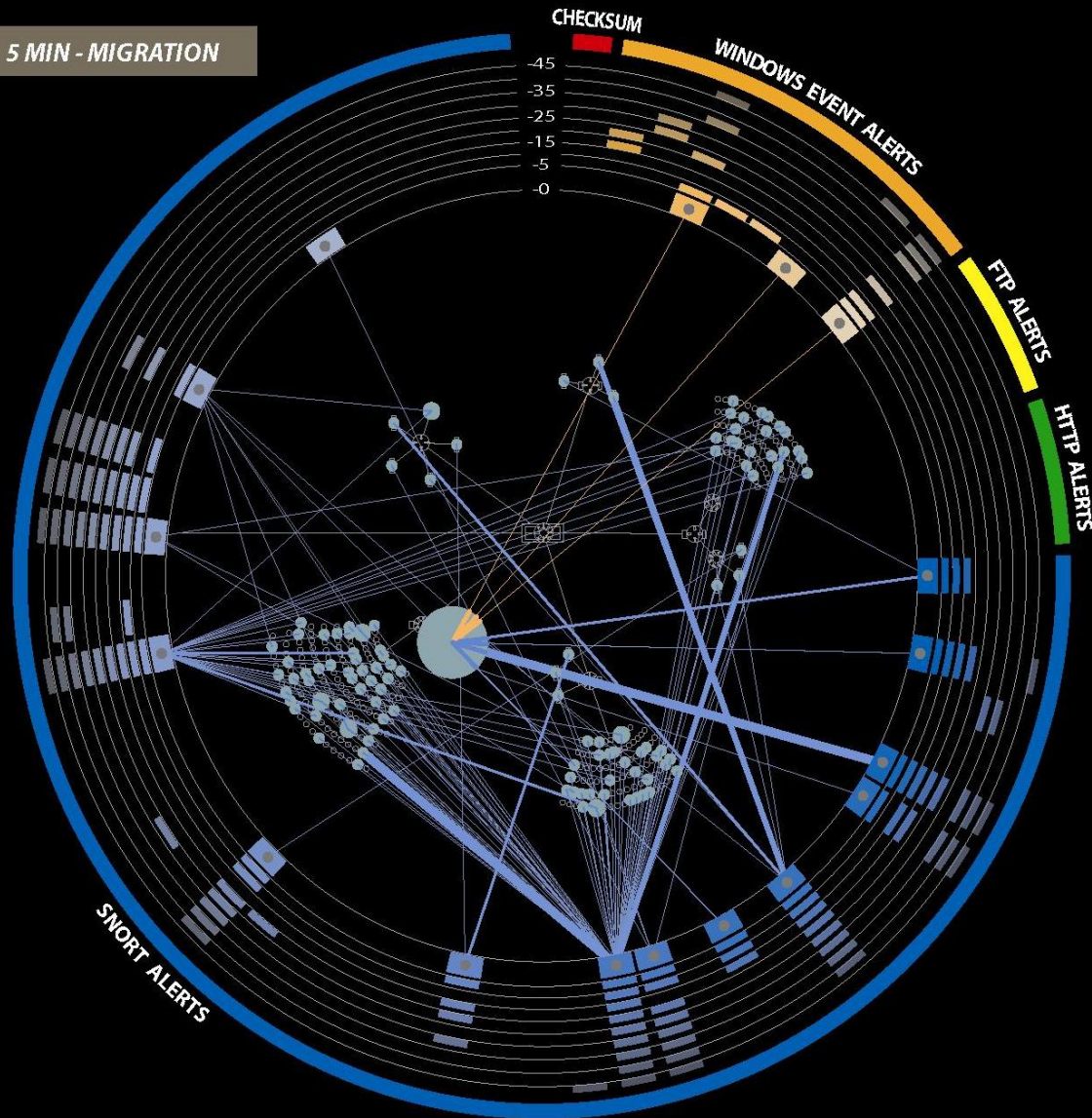
- Meeting Scheduler

- Facilitates meeting scheduling
- Patent Filed
- Prototype Prepared
- Partners Identified



# VisAlert

5 MIN - MIGRATION



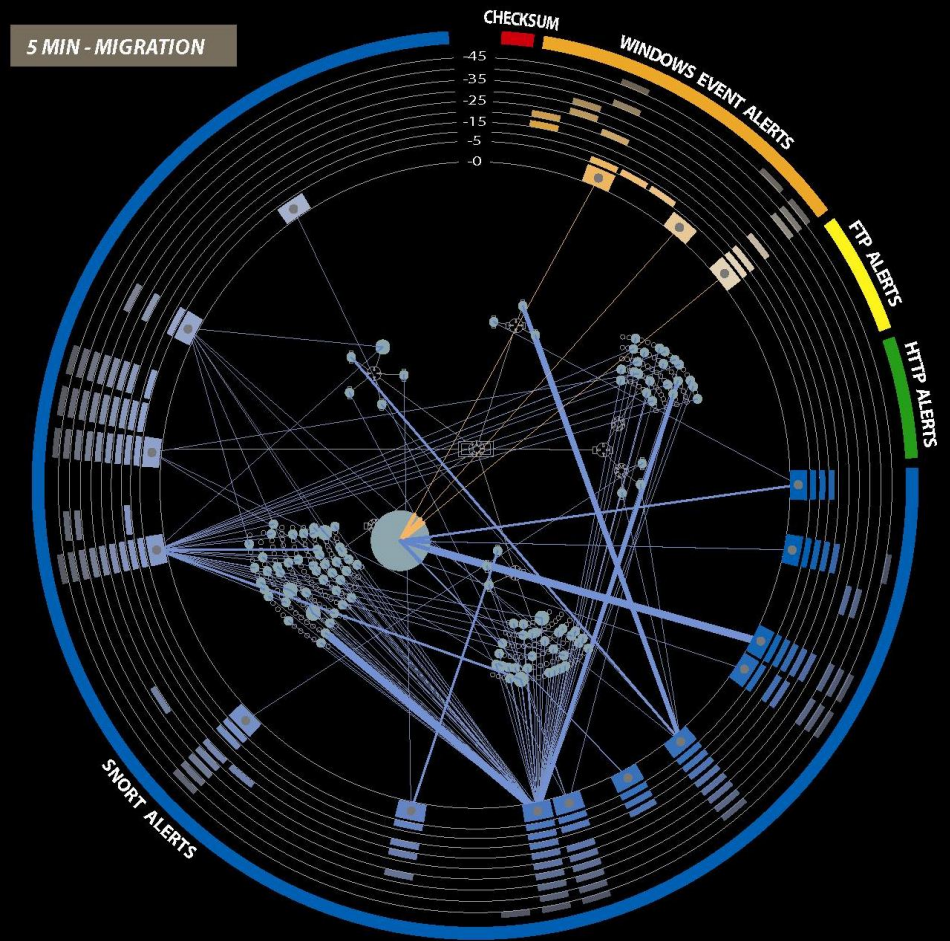
# Existing Technologies

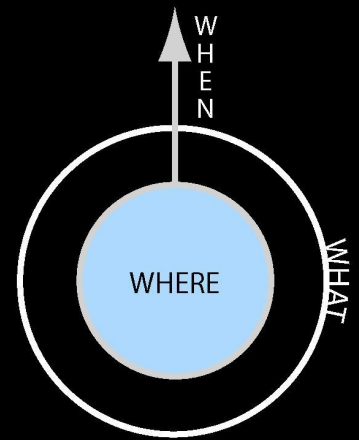
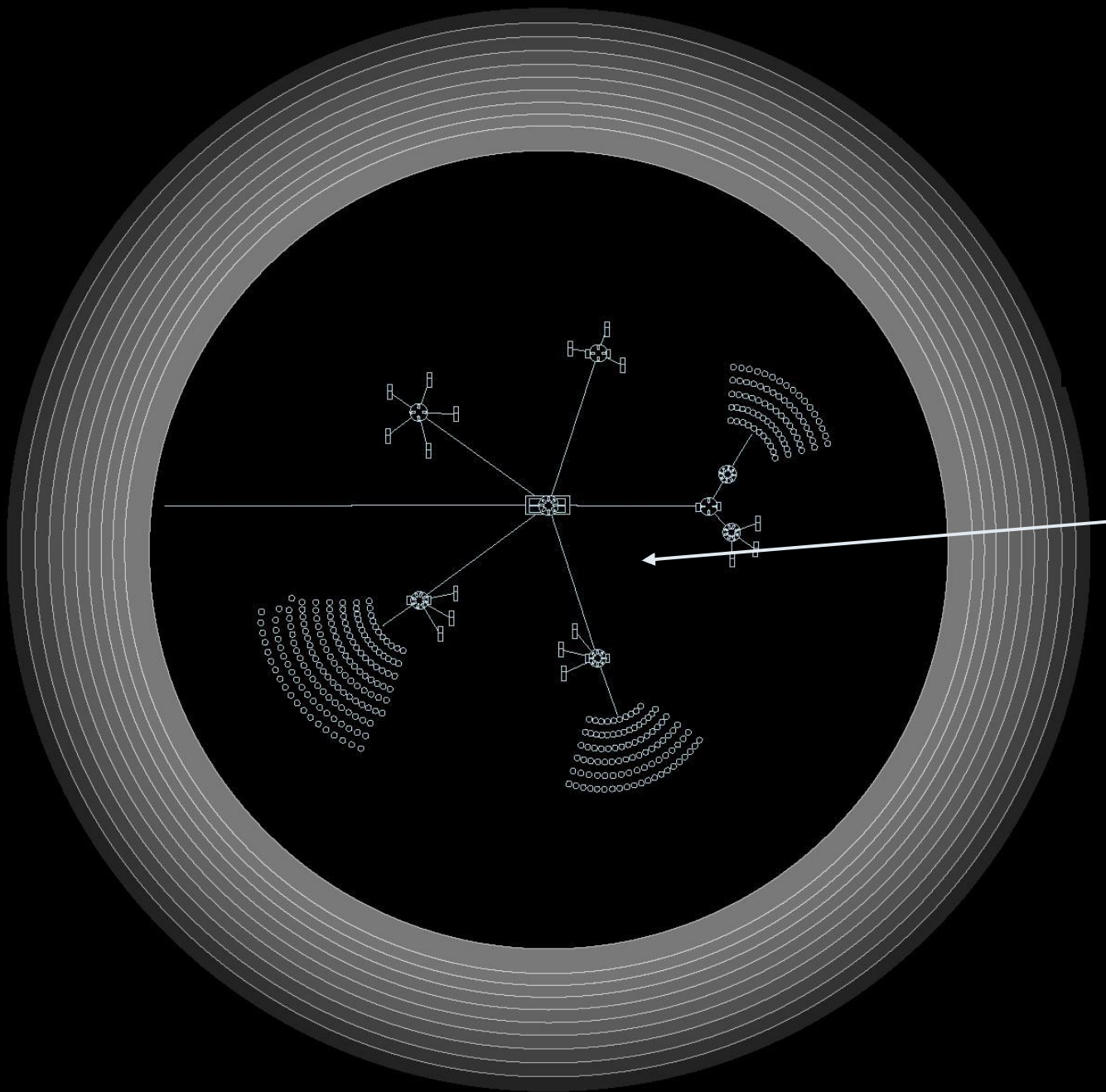
- Text based
- Inconsistency of interfaces
- Stored in different locations
- Single Sensor Single Indicator
- No holistic security view
- Difficult to query
- Time consuming
- Reactive

The image displays two screenshots of existing security technologies. The top screenshot shows the 'EventSentry: 3 in Application' window, which lists network events with columns for No., Time, Source, and Destination. The bottom screenshot shows a 'Logfile.txt - Notepad' window displaying a detailed log of a 'TestLogger' application, including source, method, date, time, computer, and stack trace information.

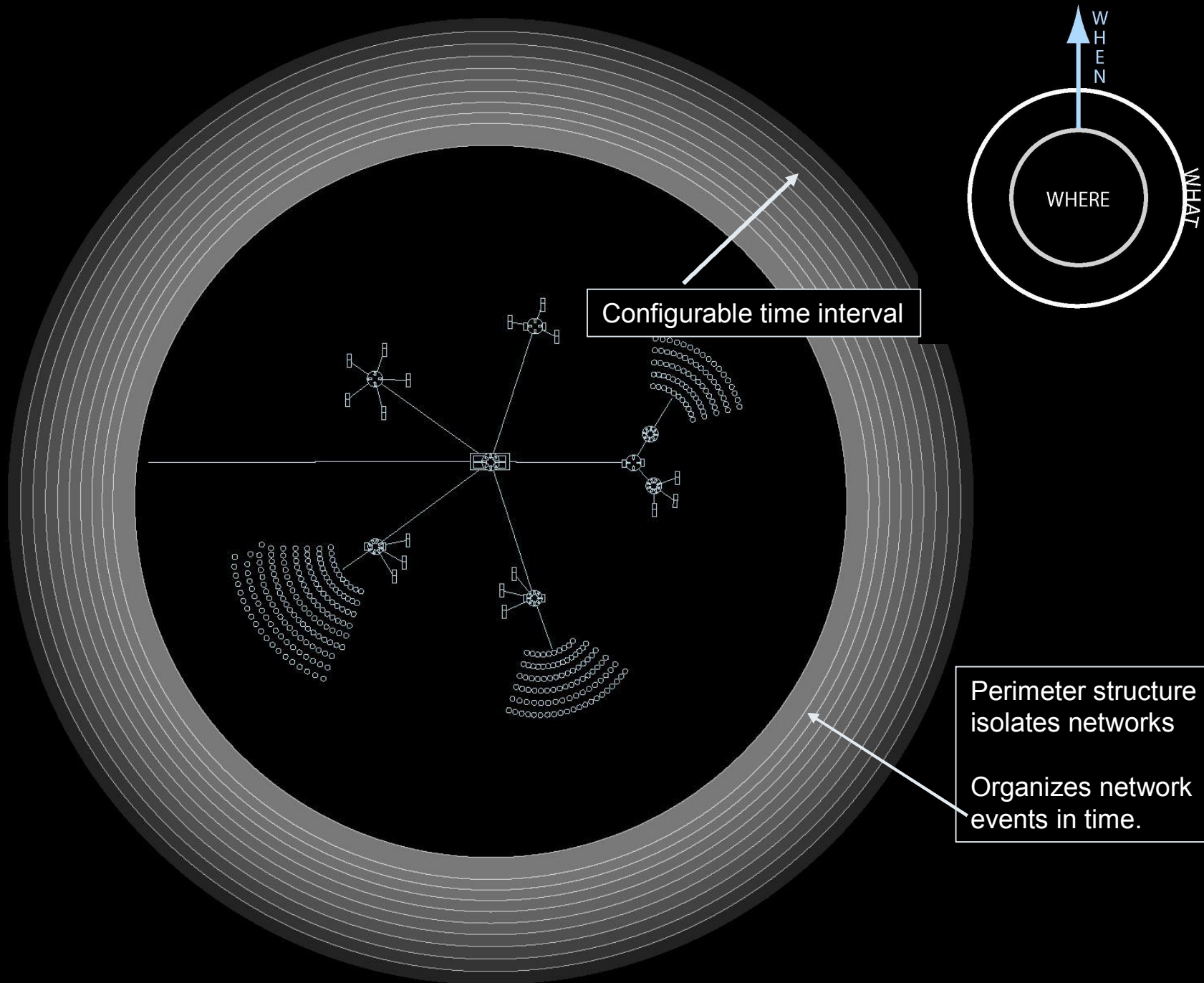
# VisAlert

- Visual correlation of disparate network alerts and logs
  - Visual Correlation
  - Emergent features
  - Query multiple databases
  - Holistic view of security status
  - Network Topology view
  - Generates queries
  - Proactive





Topology Map  
servers, switches,  
routers,  
workstations



Color indicates  
class of alert

SNORT ALERTS

CHECK  
SUM

WHERE

WHEN

WHAT

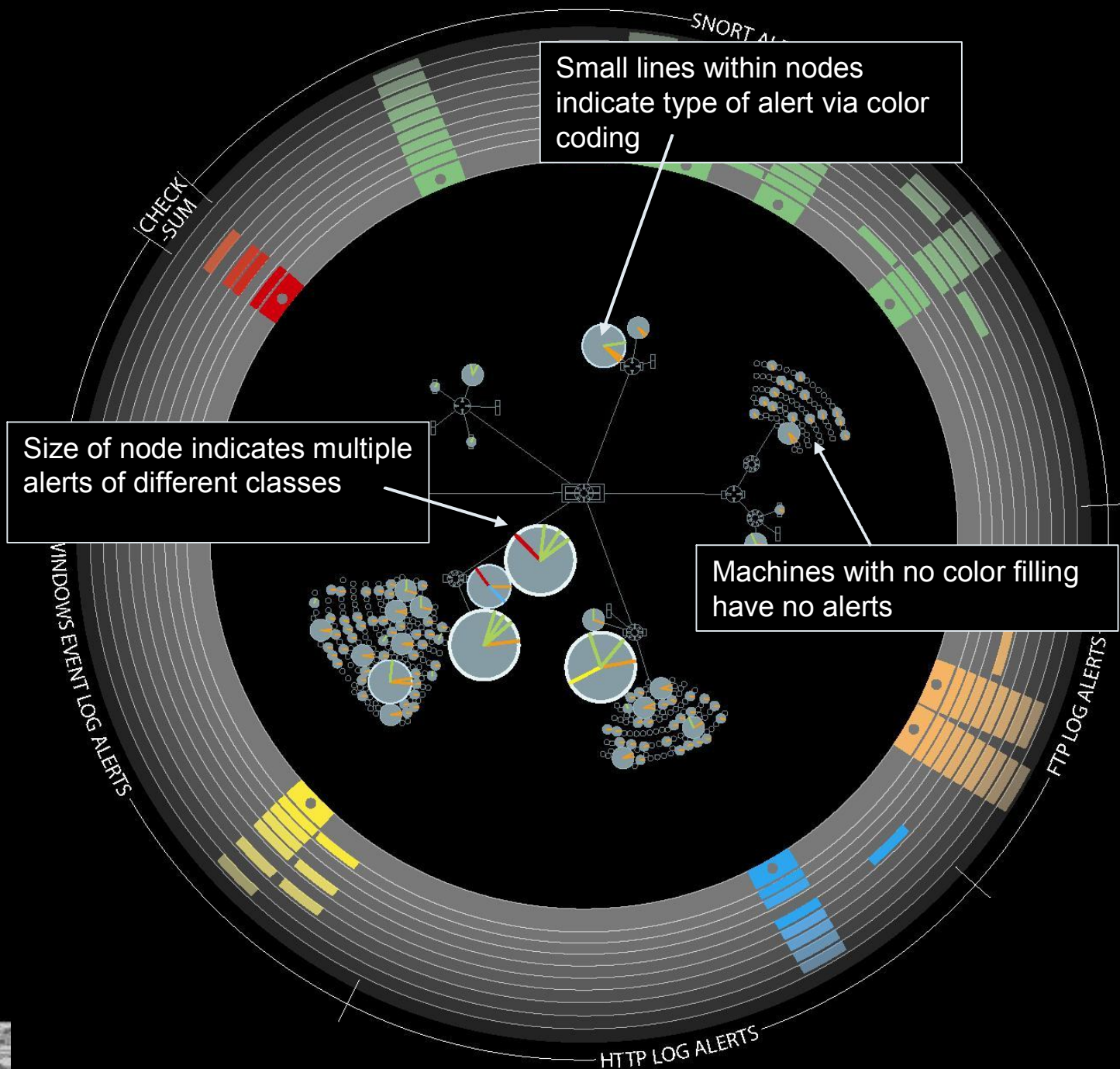
FTP LOG ALERTS

HTTP LOG ALERTS

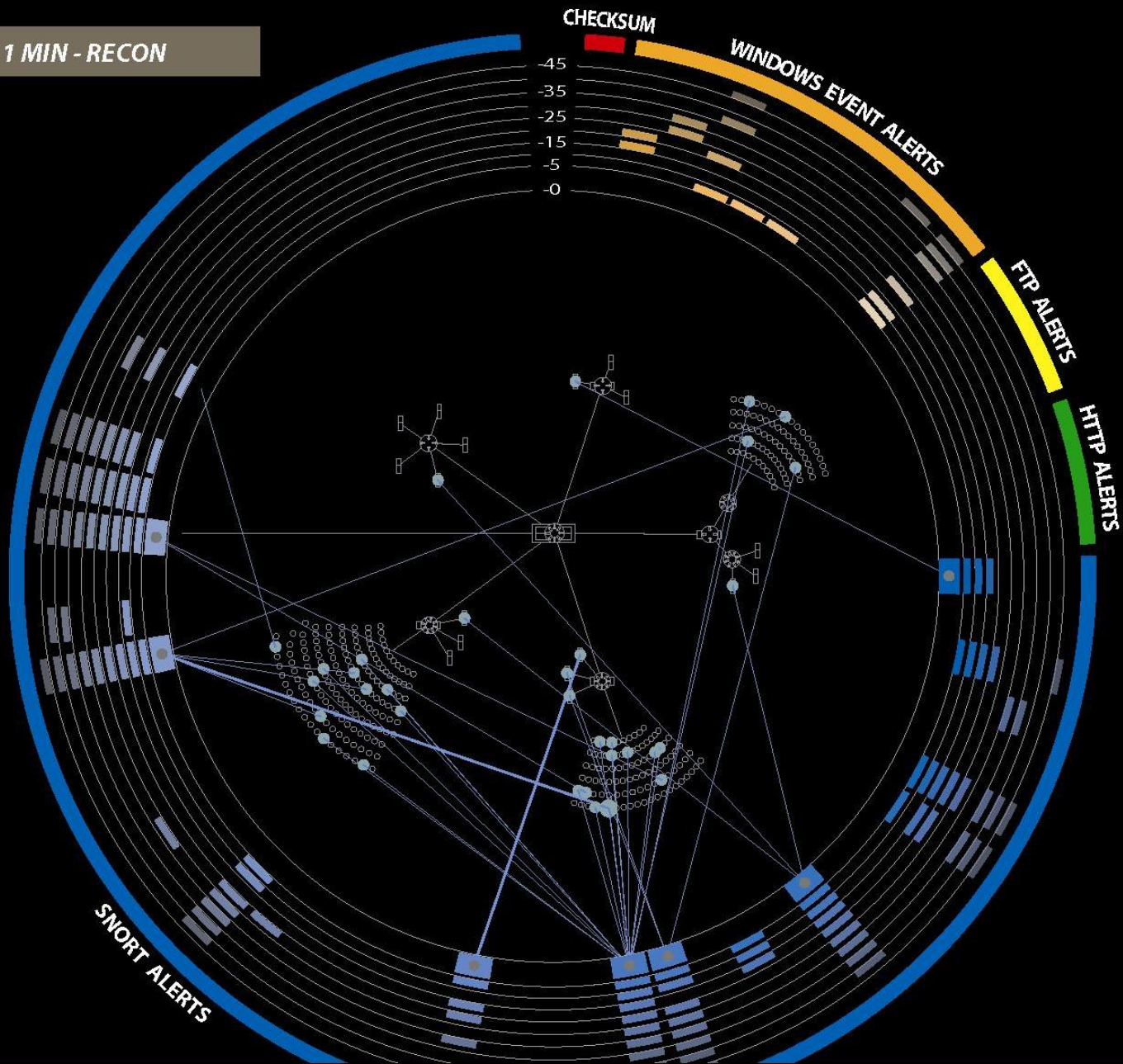
WINDOWS EVENT LOG ALERTS

Configurable set of  
alerts (logs, views)

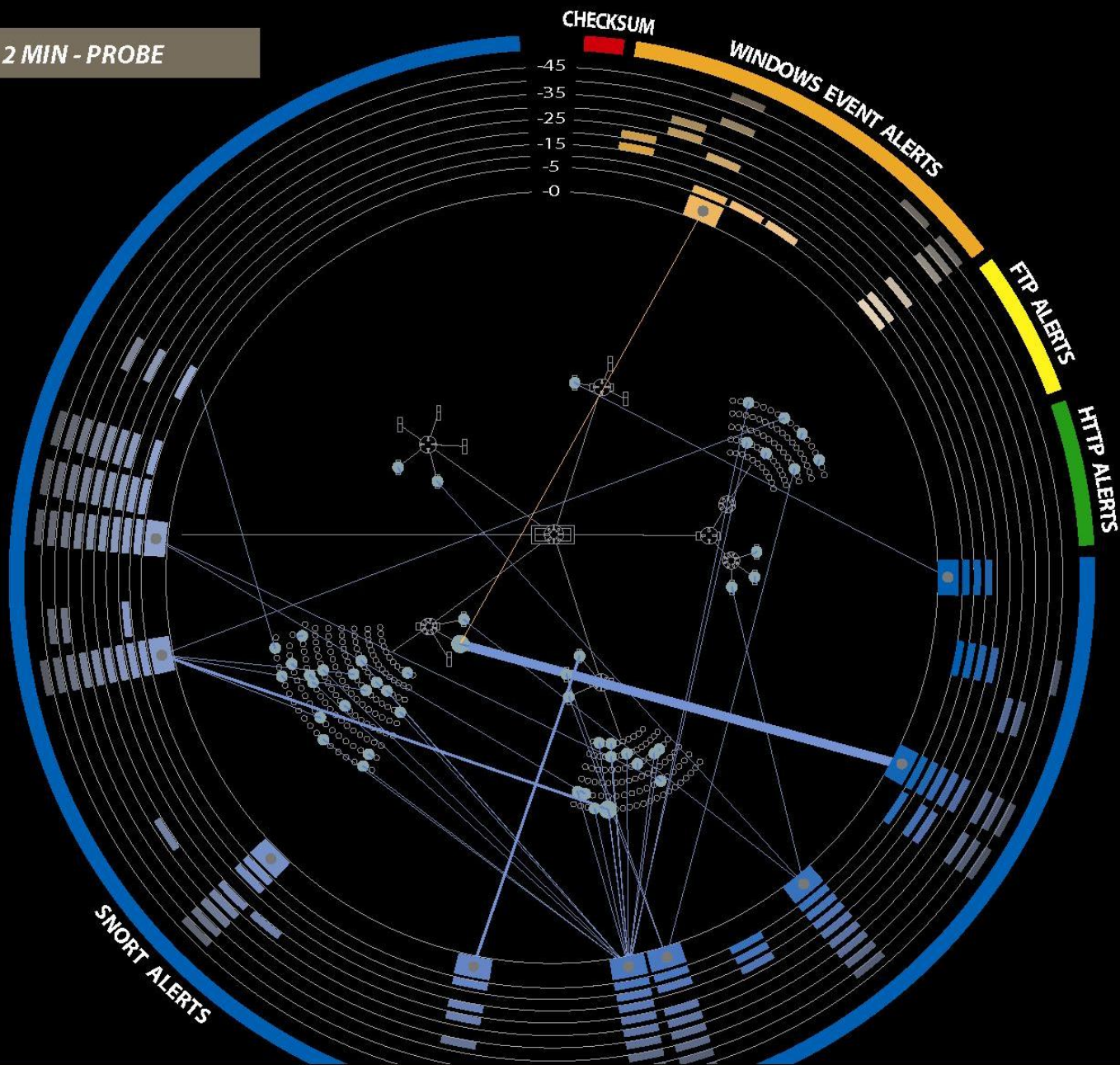




1 MIN - RECON

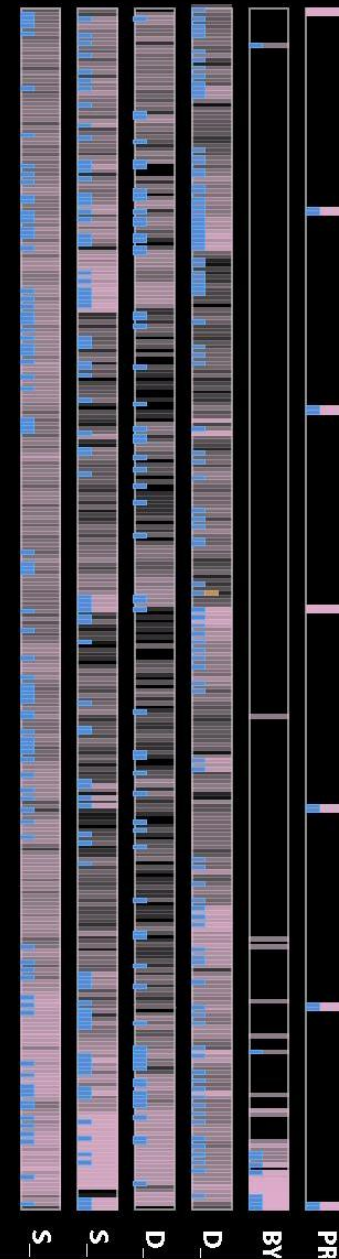
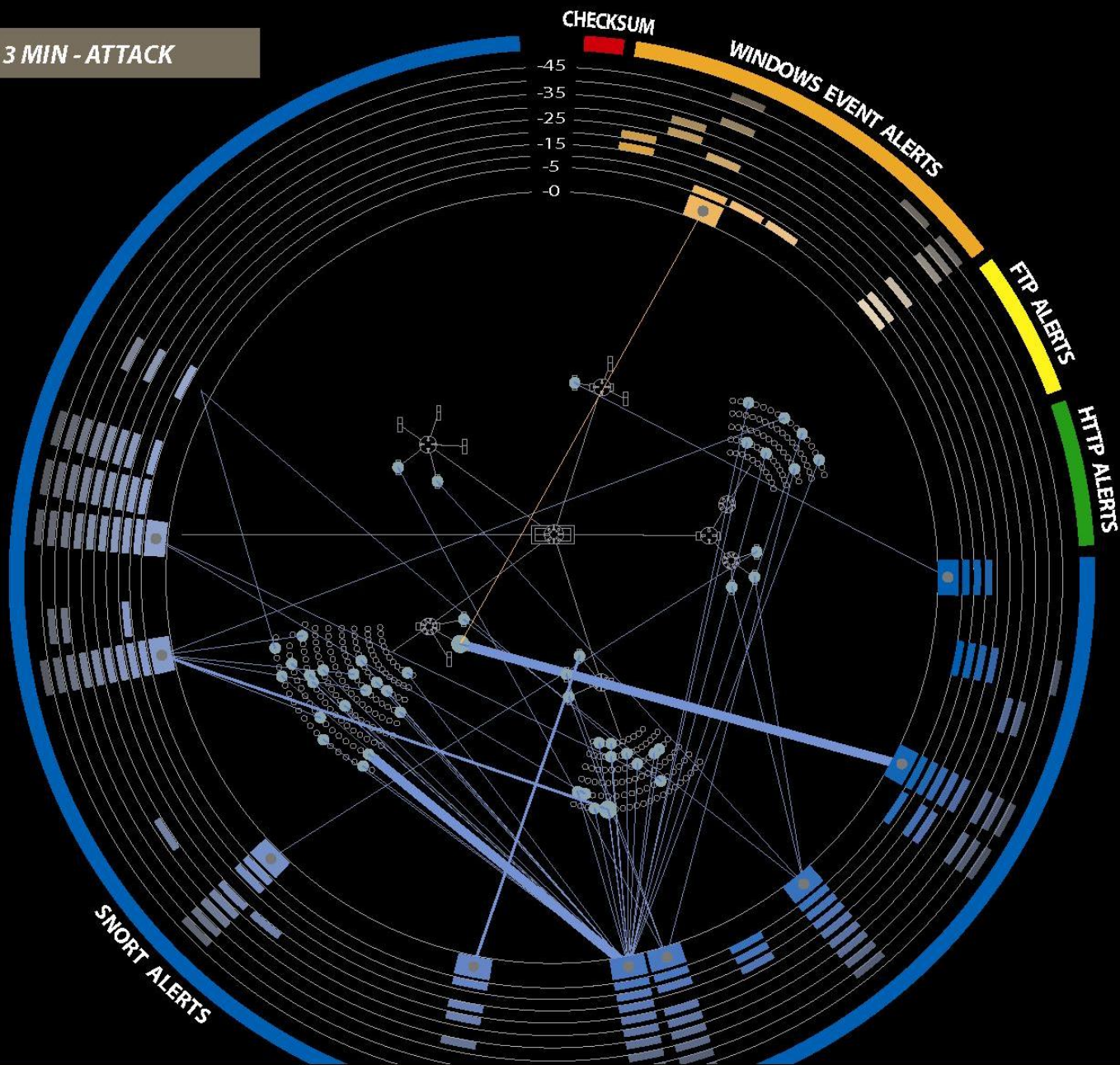


2 MIN - PROBE



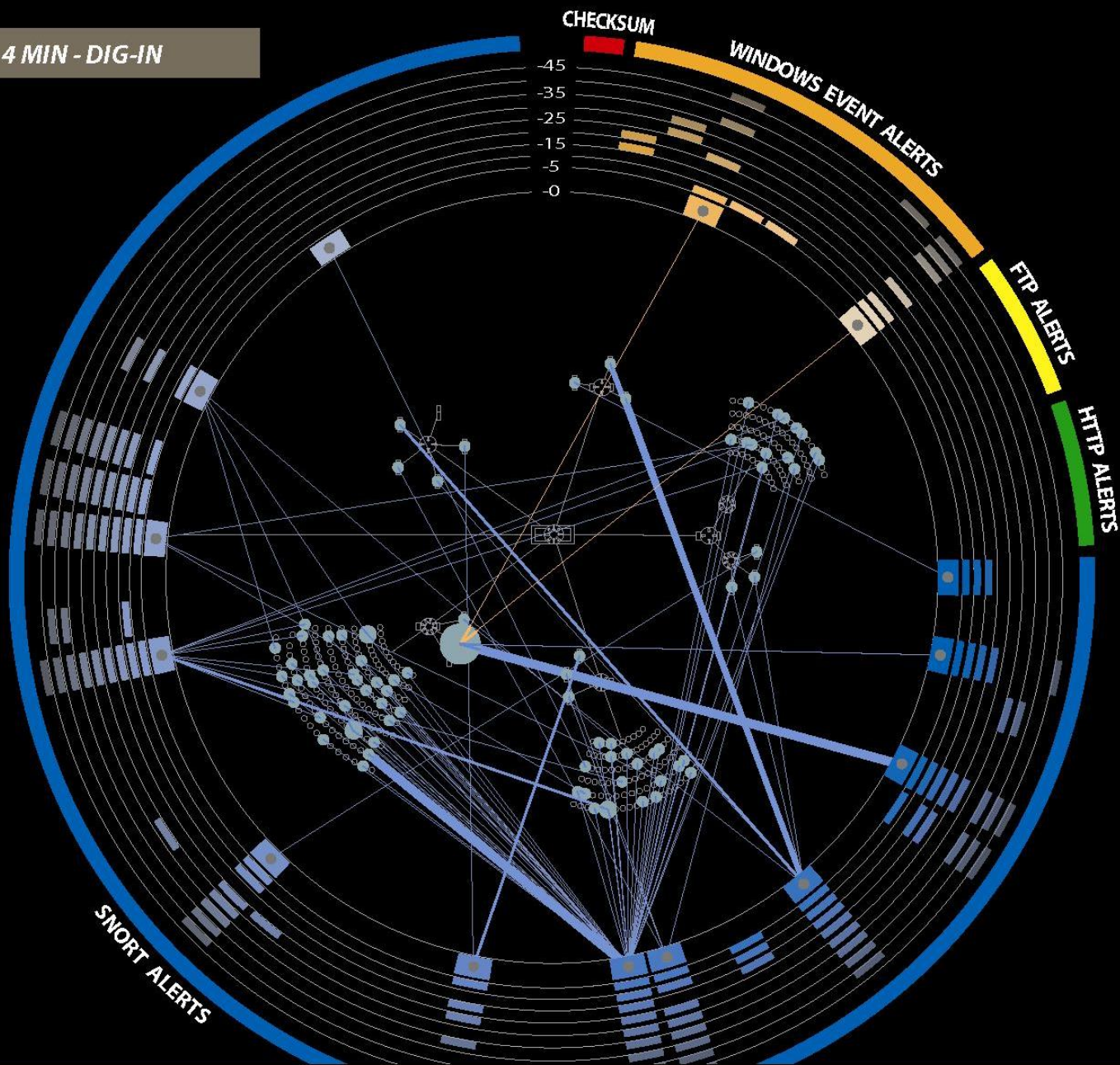
Connection to the IPC\$ interface shown with higher priority snort alert and Windows VMTools alert shown

3 MIN - ATTACK

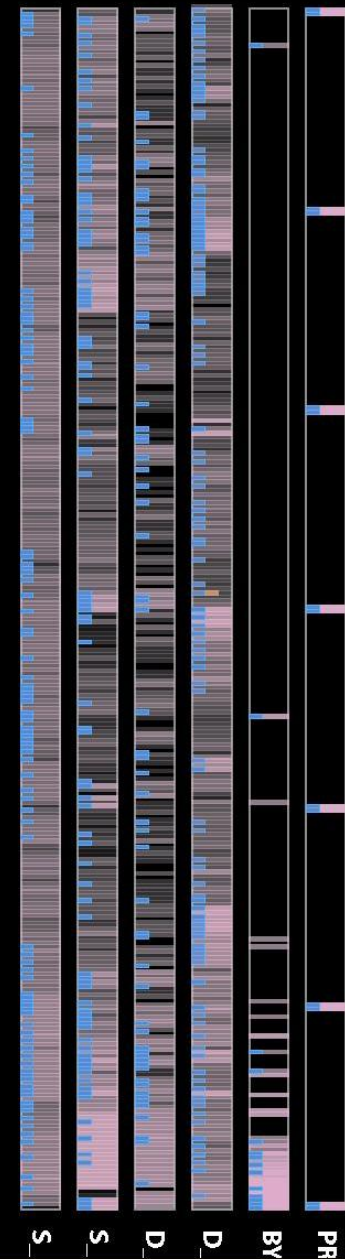


Exploitation of a vulnerability in the Windows LSASS service shown in the Windows Event Alerts

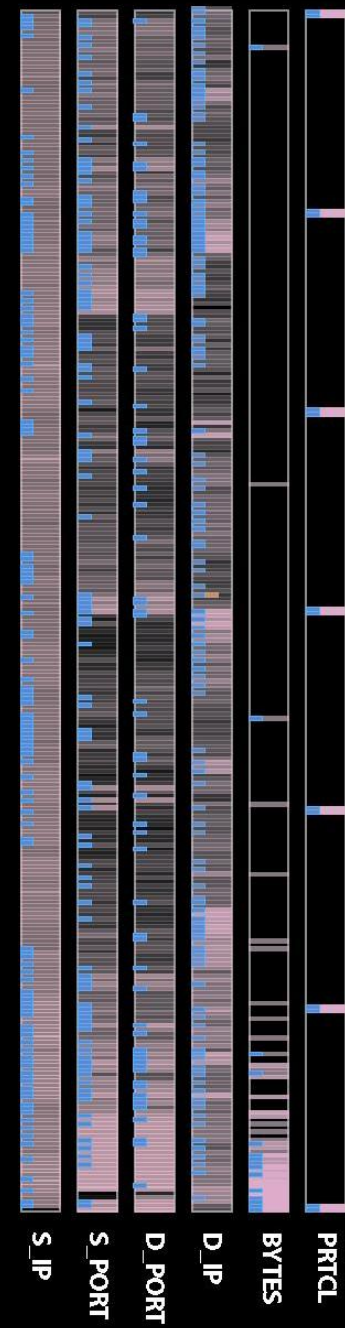
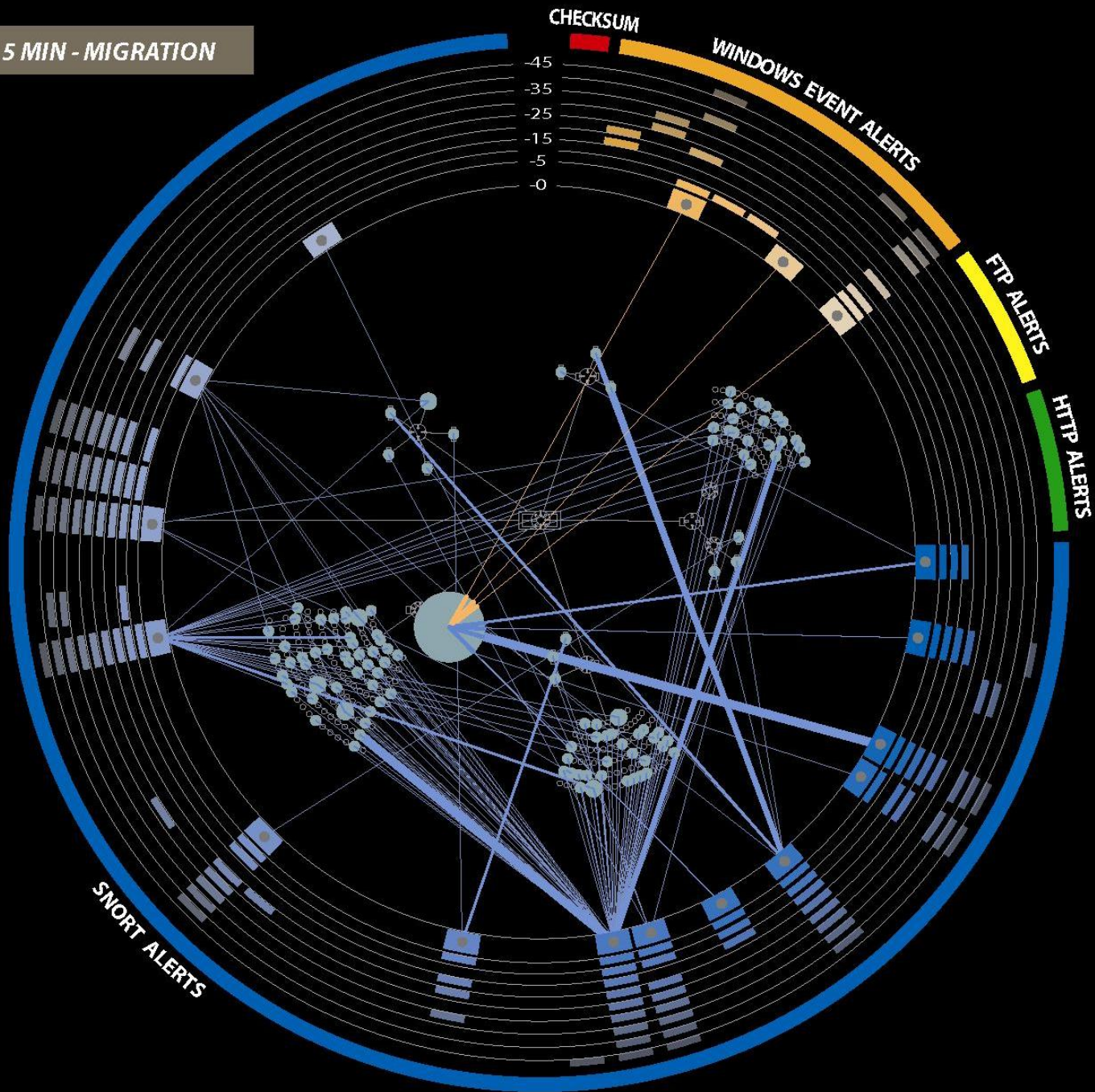
#### 4 MIN - DIG-IN



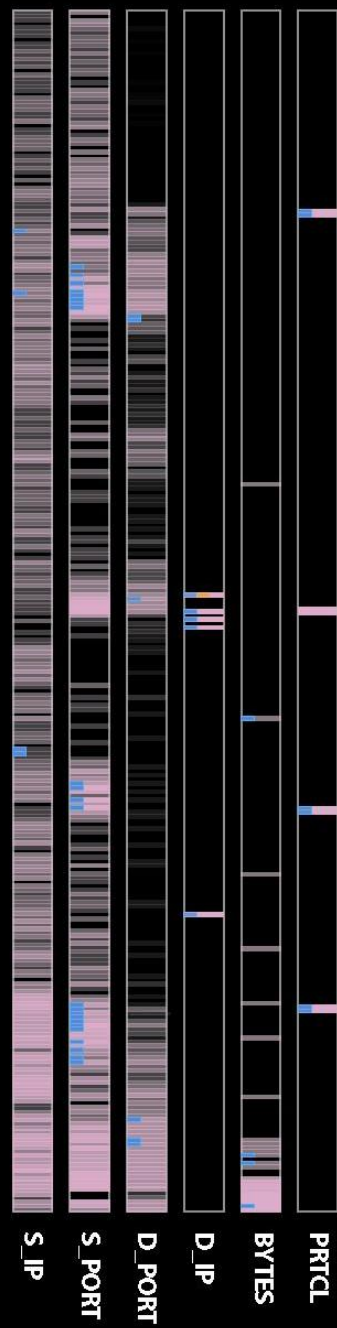
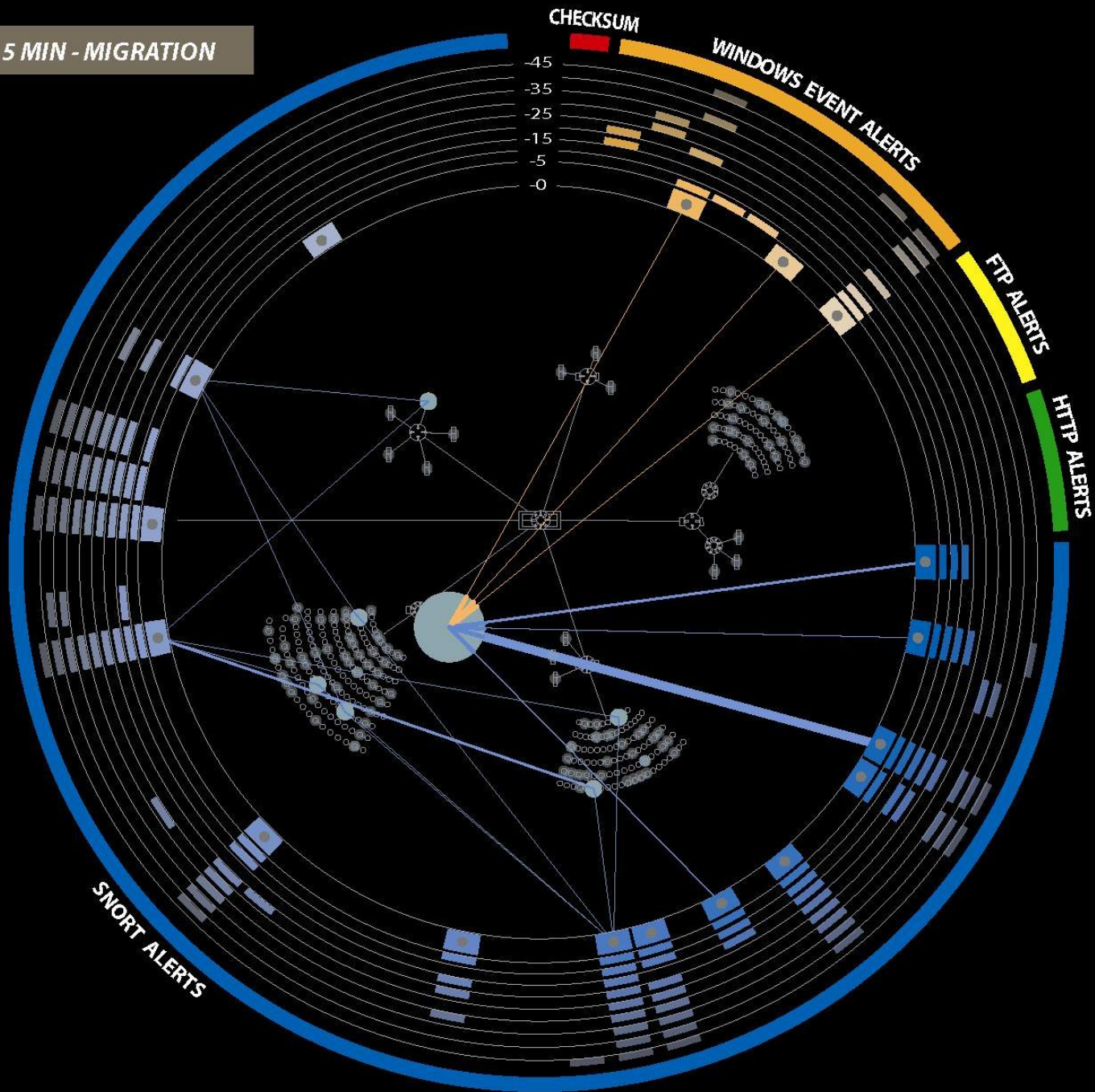
*TFTP GET command shown on snort alerts and LSASS alert in windows event log*



5 MIN - MIGRATION



5 MIN - MIGRATION





# User Feedback

- Michael Alpaugh, Marketing Manager, Computer Sciences Corporation  
“Where do I get it?”
- William Meskill, Deputy Director - DOD Joint Task Force - Global Network Operations  
“This could really help us.”
- Pete Ashdown, Xmission  
“This has a huge market.”
- Tony Sager, Deputy Chief - Defensive Information Operation Group, National Security Agency  
“ I have 3 projects for this technology.”
- David Huth, ISO U of U  
“This is a great product.”

# Competitor Comparison

	CERT/CC ACID	CROMDI VisAlertr	GUIDANCE SOFTWARE EnCase Enterprise	eIQ NETWORKS Network Security Analyzer	TENABLE Lightning	ARCSIGHT ESM 3.0	TECHNOLOGY PATHWAYS Prodiscover Incident Response
price	free	\$500	\$900	\$900	\$1000*	\$1000*	\$6000
system status view	●	●	●	●	●	●	●
scalable enterprise analysis	●	●	●	●	●	●	●
flexible trending analysis		●					
configurable log integration	●	●		●	●	●	●
real time analysis		●	●	●	●	●	●
automated analysis							●
analysis management		●				●	●
visual filtering		●					
false positive elimination		●		●			

# Market VisAlert/NOCC

Number of Employees	Number of Companies	Number of Machines in an company	Ratio of Admin to machines	Total Units	Market with \$500 per seat
			1 to 100		
100 - 500	82,334	250	3	205,835	\$102,917,500
500 - 900	8,326	750	8	62,445	\$31,222,500
1,000 - 2,499	4,995	1750	18	87,413	\$43,706,250
2,500 - 4,998	1,727	3500	35	60,445	\$30,222,500
5,000 - 9,999	884	7500	75	66,300	\$33,150,000
10,000 +	913	10000	100	91,300	\$45,650,000
				<b>573,738</b>	<b>\$286,868,750</b>

Network Operation & Control Centers (NOCC's)	Two Seats per NOCC	Total Units	Market with \$1000 per seat
20,000	2	<b>40,000</b>	<b>\$40,000,000</b>

**Totals**

**613,738**

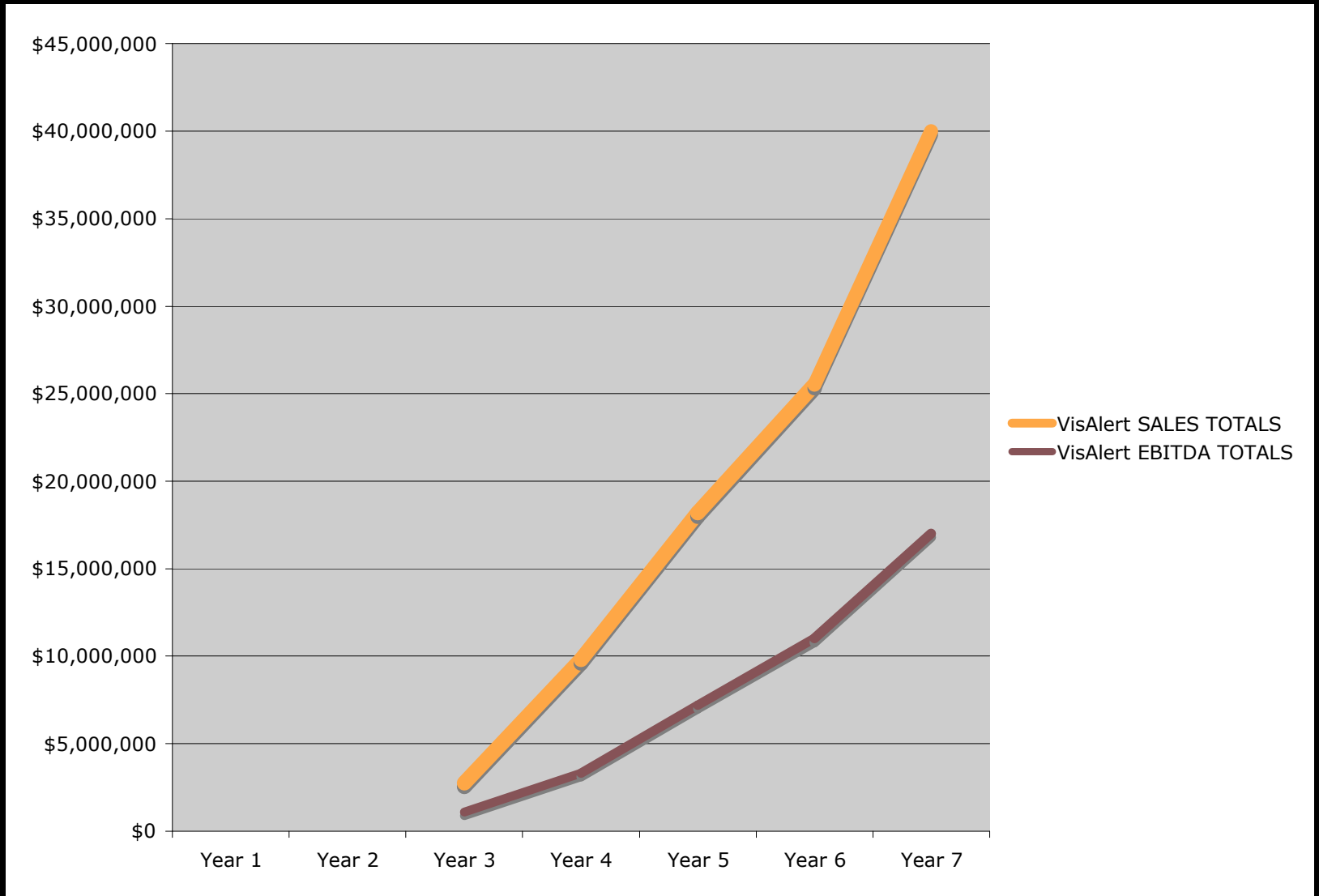
**\$326,868,750**

Source: 2002 US Economic Census

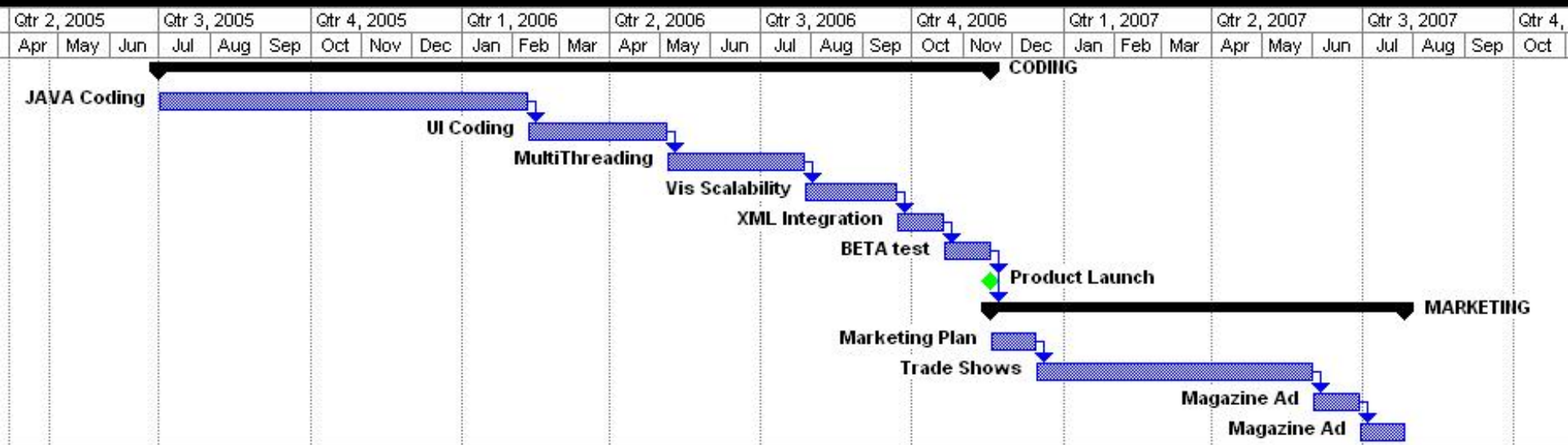
# Market Strategy

- Targeted for Network Administrators and Network Operation managers
- Web Distribution for VisAlert/NOCC
- Trade Shows
  - Information Assurance
- Magazine Ads
  - Network World

# Financial VisAlert

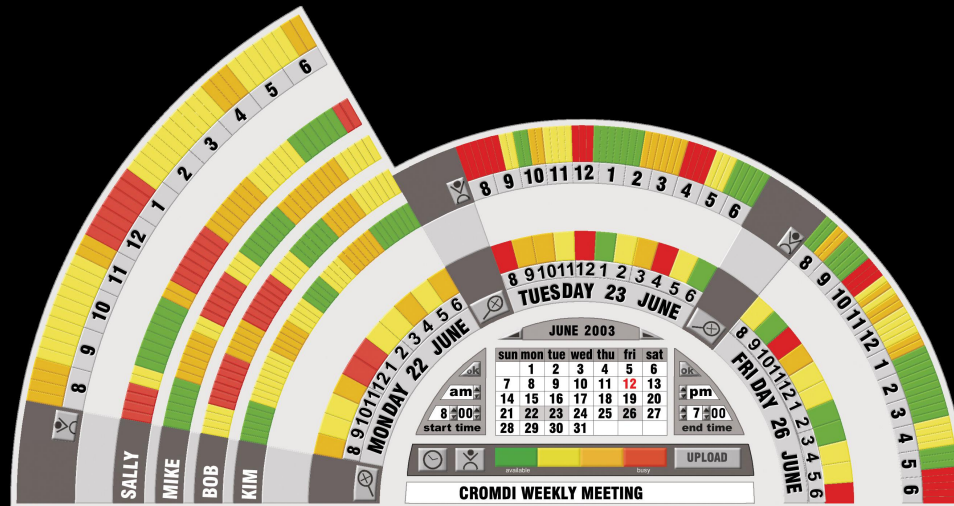
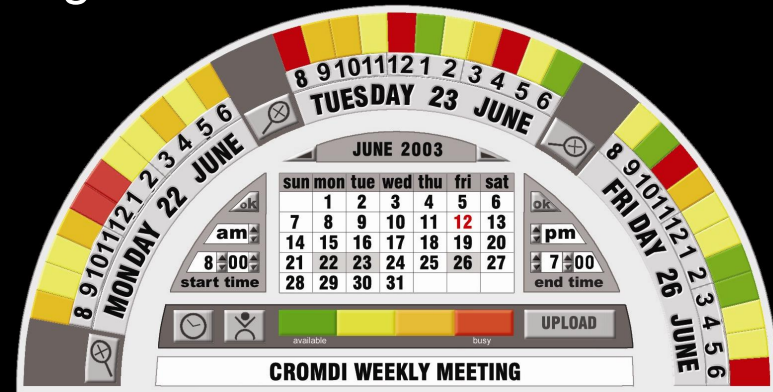


# Development Schedule



# Meeting Scheduler

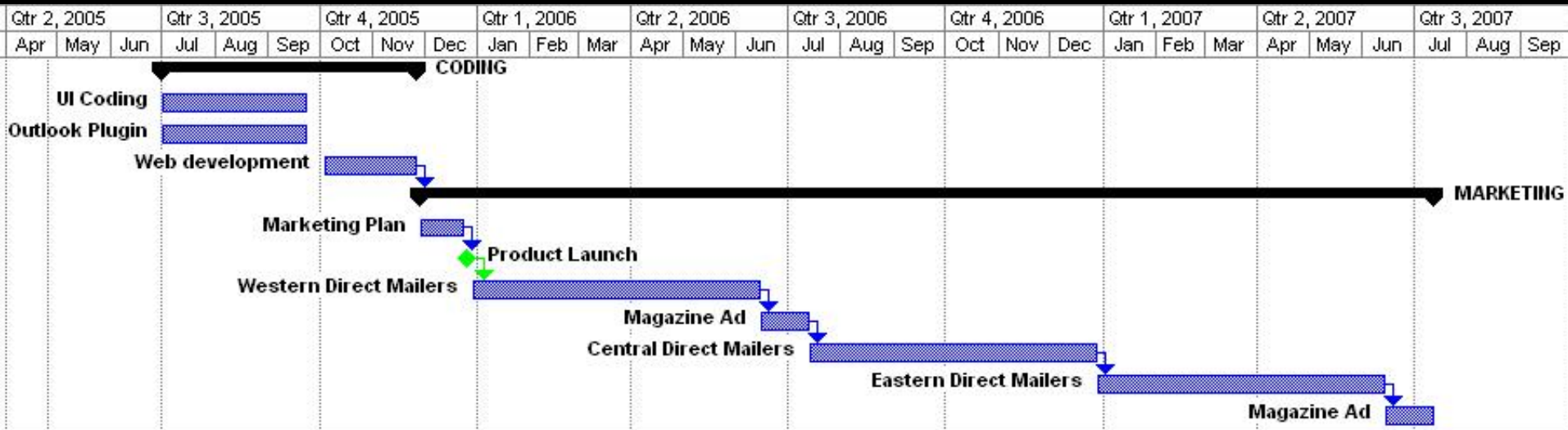
- Algorithm based visual indicator of best meeting times
  - Automated conclusion
  - Different relevance for attendees
  - Availability shading



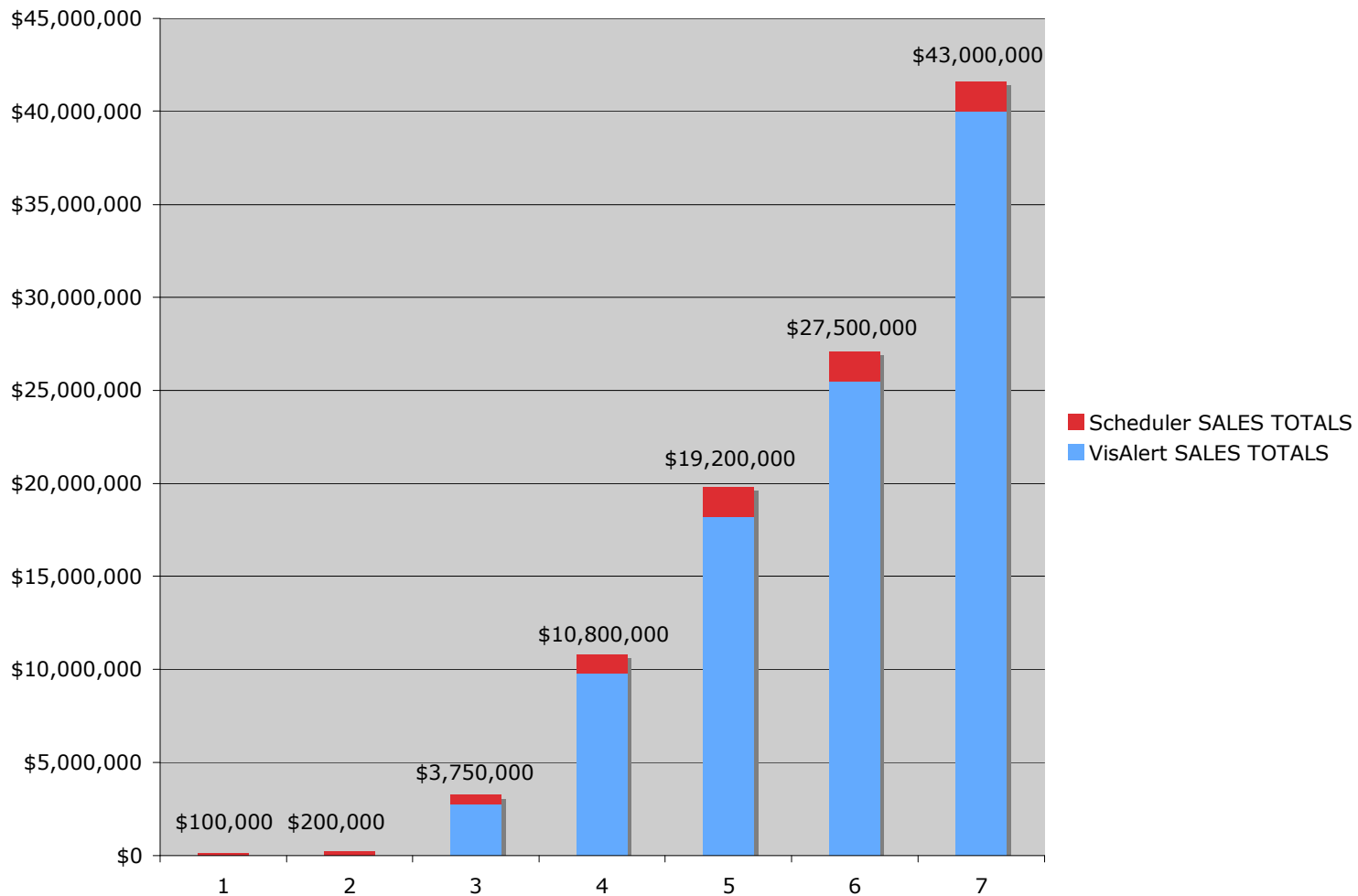
# Scheduler Summary

- Focus group indicate high demand
- Niche Market
- \$70 Million Total Market
- 6 month product launch - Near term cash flow
- Web Distribution

# Development Schedule



# Financial Summary



# Use of Funds

	Phase I		Phase II
<b>COE Funding</b>	\$100,000		
<b>Investment Funding</b>	\$600,000		\$1,000,000
<b>Totals</b>	<b>\$700,000</b>		<b>\$1,000,000</b>

# Interdisciplinary Team

Jim Agutter  
Stefano Foresti  
Julio Bermúdez  
Yarden Livnat  
Dale Richards  
Dwayne Westenskow  
Liz Tashjian  
Noah Syroid  
David Strayer  
Frank Drews

Architecture, University of Utah  
CHPC, University of Utah  
Architecture, University of Utah  
SCI Institute, University of Utah  
State COEP Consultant  
Department of Anesthesiology, University of Utah  
Department of Finance, University of Utah  
Department of Anesthesiology, University of Utah  
Department of Psychology, University of Utah  
Department of Psychology, University of Utah

External Collaborators  
Robert Urbacher  
Steve Lehman  
Matt Weinger

Utah State University  
Utah State University  
University of California San Diego

# Summary

- 3 Products
  - Meeting Scheduler
  - VisAlert
  - VisAlert NOCC
- Market Size \$400 Million
- Cumulative 7 year EBITDA \$43 Million
- \$100,000 COE
- \$1.7 Million in phase I and phase II funding
- First product in 6 months